

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA FOR
AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

MISC. NO. 2:20-mj-624-EPD

Filed Under Seal

**APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)**

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Oath Holdings, Inc (formerly Yahoo! And hereinafter “Oath Holdings”), an Internet service provider, located in Sunnyvale, California to disclose certain records and other information pertaining to the Oath Holdings account(s) pertaining to the following email addresses: bqtian@yahoo.com as described in Part I of Attachment A. The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. The Federal Bureau of Investigation (FBI) is currently investigating Baiqiang TIAN and other known and unknown persons for possible violations of 18 U.S.C. § 793 (Gathering, transmitting or losing defense information) and 18 U.S.C. § 1001 (Making false statements).

2. TIAN is a nationalized U.S. Citizen, who was born in Guanghan, China. TIAN is a Ph.D. Radio Frequency (RF) Engineer, who has been employed at Company 1, known to the Government, since approximately September 2019. Company 1 is a Cleared Defense Contractor (CDC) that works on classified research and development for the United States Government.

TIAN was hired by Company 1 as an EW (Electronic Warfare) Principal Research Scientist. TIAN has used tianbaiqiang@gmail.com to communicate with Company 1 in furtherance of his employment, including during the recruitment process.

3. Through the course of his employment at Company 1, TIAN was sponsored for a Security Clearance with the United States Government. To apply for the Security Clearance, TIAN had to fill out a Standard Form-86 (SF-86), wherein he also listed the email address of tianbaiqiang@gmail.com. TIAN signed and certified the SF-86 on September 25, 2019.

4. Additionally, TIAN signed and certified an SF-86 on September 8, 2010 for a background investigation in connection with employment at Company 2, and which listed **Bqtian@yahoo.com**.

5. At the beginning of the SF-86, under the heading "Penalties for Inaccurate or False Statements," it states that "The U.S. Criminal Code (title 18, section 1001) provides that knowingly falsifying or concealing a material fact is a felony which may result in fines and/or up to five (5) years imprisonment. In addition, Federal agencies generally fire, do not grant a security clearance, or disqualify individuals who have materially and deliberately falsified these forms, and this remains a part of the permanent record for future placements."

6. Additionally, under the heading "Statement of Understanding," it states that "I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U.S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service." TIAN checked the box labeled "Yes" to indicate his understanding. This is the first question of the SF-86.

7. Furthermore, the last page of the SF-86 is a Signature Form that states: “My statements on this form, and on any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I further affirm that to the best of my knowledge, I have not included any classified information herein. I have carefully read the foregoing instructions to complete this form. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both (18 U.S.C. 1001). I understand that intentionally withholding, misrepresenting, falsifying, or including classified information may have a negative effect on my security clearance, employment prospects, or job status, up to and including denial or revocation of my security clearance, or my removal and debarment from Federal service.” This form was digitally signed by TIAN on or about September 25, 2019.

8. Despite these repeated warnings, the evidence gathered to date indicates that TIAN provided false statements or misrepresentations in two primary areas of the SF-86. The first area of misrepresentation relates to Section 13A – Employment Activities, wherein TIAN was instructed to “(L)ist all of you employment activities, including unemployment and self-employment, beginning with the present and working back 10 years.” An Ohio Business Records Search showed TIAN as the registered agent for three active companies in Ohio, all of which were formed since 2011: AMCOM Healthcare Furniture LLC (AMCOM), Antenna Matrix LLC (Antenna Matrix), and General EM Technologies LLC (EM Technologies). TIAN listed only Antenna Matrix on his SF-86; TIAN did not list his other companies.

9. Investigators also have learned that the website www.AntennaMatrix.com is an invite only website, which means that the site owner must grant permission to a user/customer to gain access to the website. The invite only status of the website is of particular interest given the

sales and consulting nature of the business, which would normally benefit more from a website open to the public. On his SF-86, TIAN listed antennamatrix@gmail.com as his email address relating to his self-employment at Antenna Matrix.

10. The second area of false statements or misrepresentations relates to the following question on the SF-86: "Has the U.S. Government (or a foreign government) **EVER** investigated your background and/or granted you a security clearance eligibility/access?" TIAN answered "No." Yet, TIAN signed and certified an SF-86 on September 8, 2010 for a background investigation in connection with employment at Company 2, also a CDC. Furthermore, TIAN was interviewed as part of the 2010 background investigation for a security clearance. Thus, TIAN was fully aware of previously having his background investigated by the U.S. Government, yet falsely stated "No" on the SF-86.

11. Additionally, on the 2019 SF-86 as issue, TIAN listed that his dates of employment with Company 2 were from August to September 2010. TIAN also stated his reason for leaving Company 2 was "to return to my consulting business." TIAN's answer as to why he left Company 2 was also a false statement or representation. Specifically, in an interview conducted by the FBI on January 14, 2011, TIAN stated he was "let go" by his employer (Company 2) due to his inability to obtain a security clearance. Also, in an interview conducted by the FBI on August 24, 2020, a representative of Company 2 stated TIAN was discharged by Company 2 due to the uncertainty of TIAN's ability to obtain a security clearance and the potential amount of time it would take for TIAN to obtain a security clearance.

12. Finally, the FBI is investigating TIAN's potential involvement with the gathering, transmitting or losing of defense information. Such concerns have been raised in the past, to include Confidential Witness (CWD), a Facility Security Officer (FSO) at Company 2, who

confirmed that TIAN “started asking a teammate for ITAR [International Traffic in Arms Regulations] information that was outside of his scope of work, which raised red flags to both his teammate and our security group. An investigation proceeded and the employee was eventually terminated.” In 2012, TIAN also reached out to his former employer, Company 2, with a pitch for his company, Antenna Matrix, and his interest in possible contracts or consulting. He inquired about any projects Company 2 may have involving antennas. Out of an abundance of caution and given the nature of TIAN’s termination from Company 2, the email was passed to the Defense Security Services to make them aware of the contact.

13. On or about August 21, 2020, a preservation letter was submitted to Oath Holdings on **bqtian@yahoo.com**.

REQUEST FOR ORDER

14. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the United States requests that Oath Holdings be directed to produce all items described in Part II of Attachment A to the proposed Order.

15. The United States further requests that the Order require Oath Holdings not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order for a time period of one year. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant,

subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the attached court order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached court order will seriously jeopardize the investigation or unduly delay a trial, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, or change patterns of behavior.

16. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

DAVID M. DEVILLERS
United States Attorney

s/ S. Courter Shimeall
S. COURTER SHIMEALL (0090514)
Assistant United States Attorney
303 Marconi Blvd, Suite 200
Columbus, Ohio 43215
Office: (614) 469-5715
Fax: (614) 469-5653
E-mail: courter.shimeall@usdoj.gov

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following email account(s): bqtian@yahoo.com.

II. Records and Other Information to Be Disclosed

Oath Holdings is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period January 1, 2010 to present.

A. The following information about the customers or subscribers of the Account:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, **[the following items apply only to cell phones:]** Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

- B. All records and other information (not including the contents of communications) relating to the Account, including:**
- 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses; and**
 - 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).**